REMARKS

Claims 1, 2, 4 and 5 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Vanstone (US 6,195,433), in view of Schneier (Applied Cryptography), in further view of Matyas (6,307,938). Applicant respectfully traverses the rejections as follows.

Vanstone teaches a private key validation scheme that comprises generating a private key from a random number and testing the number against a predetermined set of criteria. As noted by the Examiner, Vanstone teaches generating a seed value, hashing the seed value and then shaping the output of the hash to be used as a private key. The Examiner acknowledges that Vanstone does not teach accepting/rejecting the key based on an order q. However, the Examiner turns to Schneier and Matyas as teaching accepting/rejecting a key based on an order q.

Upon a careful review of Vanstone (as explained below), it is clear that not only does Vanstone not teach choosing a key that is less than q but there is clear direction to do the opposite. Also, even if, for the sake of argument, one were to combine Vanstone with either or both Schneier and Matyas, neither Schneier nor Matyas teach testing an output to be used as a key if the value is less than an order q.

As Applicant has noted several times in previous responses, the present application describes and claims a method of generating a key that avoids the bias discovered by Daniel Bleichenbacher. The inventors have recognized the source of the bias, namely in how the key is chosen and have recognized that by choosing the key to be of an order less than q, the bias can be avoided.

Vanstone does not acknowledge this bias and is not concerned with choosing a key if the computed output is less than an order q. In fact, upon a careful read of Vanstone, it is clear that one of the tests for choosing the key involves validating the length of the seed (which is hashed to generate the key), to ensure that it is larger than n - the prime order of the generating point G (see col. 5, lines 16-17). Therefore, not only does Vanstone not teach determining whether to choose an output as a key based on whether the output is less than an order q, but clearly teaches adopting a criterion that looks for quite the opposite relationship. As such, there is nothing to suggest that the key be accepted if less than a prime order only to accept the seed value if it is larger than a prime order.

Notwithstanding the above, Applicant also believes that the Examiner has misconstrued

the secondary reference Schneier and the tertiary reference Matyas. In particular, the Examiner points again to page 487 of Schneier (lines 12-15). However, in this passage, Schneier teaches choosing a random value *k* that is less than *q* which is used to generate signature components r and s. Applicant believes that the Examiner has again made a leap of logic in modifying the teachings of Schneier to fit with what is missing from the primary reference Vanstone. Vanstone teaches choosing a key whereas the passage in Schneier teaches choosing a random value used in generating signature components. Schneier does not suggest that the value *k* can be used as a key. In fact, on page 487 of Schneier, the private key is said to be *x* and the public key is said to be *y*, not *k*.

In any event, Vanstone still teaches accepting a seed value used to generate the key based on the seed value being larger than an order n. As such, there would be no motivation to combine the teachings relied on by the Examiner as they would be contradictory. Moreover, there is no suggestion in Schneier that the random number *k* should be used for anything other than generating signature components r and s. Accordingly, Applicant believes that the Examiner has combined the cited references without fully considering how the respective teachings would work together. It is believed that the Examiner has read too much into the references cited on the basis of hindsight in view of Applicant's disclosure.

None of the cited references have recognized the bias recognized by the inventors let alone teach how such bias can be avoided. It is therefore believed that claims 1, 2, 4 and 5 clearly and patentably distinguish over the combination of cited references.

Claims 7-13 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Vanstone, in view of Schneier, in further view of Matyas (Vanstone/Schneier/Matyas), in further view of Backal (US 6,219,421). Applicant respectfully traverses the rejections as follows.

Backal appears to have been cited as teaching incrementing a seed value by a predetermined function. Claims 7 and 8 are dependent on claim 1, which Applicant is believed to have shown distinguishes over Vanstone/Schneier/Matyas. Therefore, Backal must at least teach what is missing from Vanstone/Schneier/Matyas. Applicant respectfully submits that Backal does not teach choosing a key based on whether or not it is less than an order q.

Therefore, Backal does not teach what is missing from Vanstone/Schneier/Matyas and claims 7 and 8 are believed to distinguish over Vanstone/Schneier/Matyas in further view of Backal. Similar arguments apply with respect to claims 9-13. As such, claims 7-13 are believed

to be patentably distinguished over the references cited by the Examiner.

Claims 3, 6 and 14 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Vanstone, in view of Schneier, in further view of Matyas (Vanstone/Schneier/Matyas), in further view of Nel (Generation of Keys for use with the Digital Signature Standard (DSS)). Applicant respectfully traverses the rejections as follows.

Claims 3, 6 and 14 are dependent on either claim 1 or claim 9, which Applicant is believed to have shown distinguish over Vanstone/Schneier/Matyas. Therefore, Nel must at least teach what is missing from Vanstone/Schneier/Matyas. Applicant respectfully submits that Nel does not teach choosing a key based on whether or not it is less than an order q. Therefore, Nel does not teach what is missing from Vanstone/Schneier/Matyas and claims 3, 6 and 14 are believed to distinguish over Vanstone/Schneier/Matyas in further view of Nel. As such, claims 3, 6 and 14 are believed to be patentably distinguished over the references cited by the Examiner.

Claims 1, 2, 4 and 5 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier, in view of Matyas, in further view of Patel (US 6,327,660)

As noted above, the present application describes and claims a method of generating a key that avoids the bias discovered by Daniel Bleichenbacher. The inventors have recognized the source of the bias, namely in how the key is chosen and have recognized that by choosing the key to be of an order less than q, the bias can be avoided.

Again, the Examiner points to page 487 of Schneier (lines 12-15) as teaching choosing a key based on a value being less than an order q. However, in this passage, Schneier teaches choosing a random value k that is less than q which is used to generate signature components r and s. The Examiner acknowledges that Schneier does not teach computing a hash of a seed value and points to Matyas as teaching such a feature. However, Applicant again points out that there is nothing in Matyas to suggest modifying Schneier such that the value k is used as a key. It is believed that the Examiner has again made a leap of logic in saying that it would be obvious to combine and/or modify these references to fit what is claimed. None of the references suggest the claimed feature of determining whether an output is less than an order q and if so, using that output as a key.

Patel teaches securing a communication link before boot. However, Patel clearly does not teach what Applicant believes is missing from Schneier and Matyas. Therefore, the arguments regarding Vanstone/Schneier/Matyas equally apply to Schneier/Matyas/Patel and

Applicant believes these rejections are no more relevant than those regarding Vanstone/Schneier/Matyas.

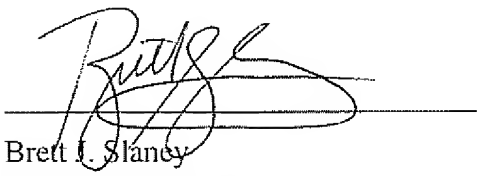
None of the cited references have recognized the bias recognized by the inventors let alone teach how such bias can be avoided. It is therefore believed that claims 1, 2, 4 and 5 also clearly and patentably distinguish over Schneier/Matyas/Patel.

Claims 7-13 have been rejected under 35 U.S.C. 103(a) regarding Schneier, Matyas, Patel and Backal; and claims 3, 6 and 14 have been rejected under 35 U.S.C. 103(a) regarding Schneier, Matyas, Patel and Nel. As noted above, the combination of Schneier/Matyas/Patel is believed to be no more relevant than the combination of Vanstone/Schneier/Matyas and, as such, similar arguments presented above equally apply in respect of claims 7-13 and 3, 6 and 14.

In view of the foregoing, Applicant believes that claims 1-14 clearly and patentably distinguish over the references cited by the Examiner and are in condition for allowance.

Applicant requests early reconsideration and allowance of the present application.

Respectfully submitted,



Brett J. Slaney
Agent for Applicant
Registration No. 58,772

Date: March 5, 2007

BLAKE, CASSELS & GRAYDON LLP
Suite 2800, P.O. Box 25
199 Bay Street, Commerce Court West
Toronto, Ontario M5L 1A9
CANADA

Tel: 416-863-2518
BSL/